6. SECURITY VIEW

This section provides a definition of the security architecture for ICS. The approach to ICS System security is done in two steps. First, an assessment of the ICS is presented. This motivates the second part which presents the system design for a secure ICS.

6.1 ICS Security Assessment

The purpose of the ICS Security Assessment is to explain the need for appropriate security risk mitigation measures addressed in Section 6.2.

6.1.1 ICS Security Needs Overview

ICS is an international catalogue interoperablity program accessible to users on a global basis. Built on an open-computing network architecture to facilitate access by a wide variety of users, the driving requirements of its security architecture are integrity, availability, and confidentiality of its data assets. The project vision is open access to well-pedigreed data in which users may have confidence, while maintaining certain proprietary and administrative data in confidence.

Integrity. Because of the scientific nature of the project, integrity of project information is critical. The accuracy of the collection, product, guide and browse data must be stored and accessed in a fashion which maintains the integrity of the data. In addition, information to support ordering of ICS products and services must be protected against unauthorized access.

Users expect the system to guard against tampering with the source materials of the *Retrieval Managers* not only during storage, but during maintenance and distribution. Integrity threats are manifested through unauthorized access or use, leading to change, alteration or modification of information resources. The security architecture must provide adequate safeguards against these threats.

Availability. The ability to have assured use of project resources is vital to instill confidence in its users. Availability needs translate into two categories: fault tolerant features to preclude failure or operational disruption; and recovery actions, to enable timely resumption of operational activities and minimize the length of the disruption. Availability threats are manifested through denial of service events, either physical in nature (e.g., fire or loss of power) or logical (e.g., computer virus or other intrusive software).

Confidentiality. Confidentiality requirements exist because some of the information within ICS requires special protection. This includes specific user product requests and account information, and information of a private nature on individual users on the system. Information of this nature, if compromised, could result in damage or harm to ICS or to individuals. Confidentiality threats are manifested through access by unauthorized persons and authorized persons who have exceeded their privileges, e.g., surreptitious monitoring of data ordering for competitive reasons.

6.1.2 Vulnerabilities

A vulnerability is a weakness in security procedures or controls that could be exploited by a threat. Vulnerabilities are often analyzed in terms of missing safeguards. Vulnerabilities contribute to risk because they may “allow” a threat to harm the system. Section 6-2, links the ICS security controls that counter the threats which may potentially exploit ICS vulnerabilities. There are seven categories of vulnerabilities which may impact ICS. They are:

Software Vulnerabilities. Software vulnerabilities include: inadequate configuration management that permits program errors; unauthorized automated routines; and inadequacies in system and application software that may result in processing or calculation errors, or may allow unauthorized access to hardware, data, or programs. Given the collaborative nature of the software development of CEOS *Retrieval Managers*, these vulnerabilities may occur due to unintentional miscommunication.

Hardware Vulnerabilities. Hardware weaknesses include: improper operation of hardware; lack of proper hardware maintenance; inadequate physical security; and inadequate protection against natural disaster. Because all ICS hardware will be procured, installed and maintained by procedures outside of ICS, it is assumed that hardware security measures will be followed at each site. The availability of the *Retrieval Manager* at each site is contingent on this assumption. The ICS security design will need to protect against breaches of confidentially and integrity to other sites independent of hardware failures at a given site.

Data Vulnerabilities. Data vulnerabilities include inadequate access control that permits unauthorized access or authorized personnel to exceed privileges with the potential result of both accidental and malicious deletion, corruption, modification, or destruction of data, as well as theft. Of special concern to ICS are susceptibilities that impact the integrity of collections data, browse and guide data held by the *Retrieval Manager*, system configuration data, registration data, authentication data, and ordering data.

Administrative Vulnerabilities. Administrative vulnerabilities are associated with weaknesses in the effective administrative control of IT resources. They include inadequate or nonexistent administrative and security policies, guidelines, training, and controls; operating procedures (i.e., standard operating practices and procedures); management constraints, and accountability. As the administration of ICS is distributed throughout its agency members, it will be assumed that the availability of each site's *Retrieval Manager* will be dependent on the site's administrative practices. Some administrative practices will be defined by the PTT, e.g. Collection Manual [R5], but their application is dependent solely on the site's personnel. ICS must protect from losses of integrity or confidentiality from a lapse in a single site's administration.

Communications Vulnerabilities. Vulnerabilities associated with communications include: inadequate access control that allows unauthorized access to networks and communications circuits that could result in transmission interception and unauthorized access to network components; and inadequate measures to prevent circuit failure from both natural disaster and human activities, intentional and accidental, resulting in denial of service. ICS is dependent upon the CEOS Network as defined by the CEOS Network Sub-group. Individual site communication security is dependent upon routers for their sites.

Personnel Vulnerabilities. As used here, the term personnel means people who have an authorized association with ICS resources or facilities, such as: employees, certain guests and maintenance personnel, and authorized system users. This group of people is often referred to as "insiders". Insiders represent the greatest weakness in any system, including ICS, because they already have access, usually understand the system configuration and operation, and may be aware of existing vulnerabilities. Security weaknesses associated with insiders include inadequate physical and logical controls that allow an insider access to systems beyond which she or he has privileges; and inadequate administrative procedures or controls to minimize or detect accidents involving IT resources or IT resource theft, abuse, misuse, damage or destruction. Perhaps the greatest weakness involving insiders is that they are exposed to external influences and pressures that may provoke malicious acts against IT resources, such as destruction or theft.

Facility Vulnerabilities. Facility weaknesses include: inadequate physical security that permits accessibility by unauthorized persons which could lead to facility, and content, misuse, damage, or destruction, or theft of its contents; and inadequate protection against natural disaster that may result in

the damage or destruction of the facility or its contents. Furthermore, poor facility maintenance and services, such as poor housekeeping, poor air quality, temperature extremes, and power fluctuations may result in damage to or destruction of IT resources.

As the ICS resources are distributed throughout its agency members, it will be assumed that the availability of each site's *Retrieval Manager* will be dependent on the site's facility practices. ICS must protect from losses of integrity or confidentiality from a lapse in a single site's facility.

6.1.3 Threats

ICS is concerned with threats that exploit the above vulnerabilities and have a detrimental impact on the integrity, availability, and confidentiality of its IT resources. Generally, threats to ICS resources come from two major sources: natural disaster and human activity.

- Natural disaster includes: airborne particles, cataclysm (earthquake, volcanic eruption, tidal wave, etc.) , fire, static electricity, and weather. Note that these threats will exploit vulnerabilities at specific sites affecting availability over which the ICS system design has no authority. But ICS must preclude lapses in confidentiality and integrity to other sites given a natural disaster, i.e. contain any threat to the single site.

- Human activity includes activity from both authorized persons and unauthorized persons.

  – Authorized persons are users, employees, and maintenance personnel who have some level of authorization to use or have access to ICS resources. Threats resulting from authorized activity may be accidental (an incident without malice) and intentional (a malicious act). This may include otherwise authorized persons who exceed their authority. This may also include errors or omissions in the software development or the intentional or accidental inclusion of malicious code, e.g. viruses.

  – Unauthorized persons are users or persons who do not have authorization to use or have access to ICS resources. Even though in theory, activity by unauthorized persons can be accidental, this section treats all such activity as intentional.

6.1.4 ICS Security Definitions

The following definitions are used in the ICS with respect to security concepts.

Authentication: Verification of the identity of a user or, validation of a communication (the second part provides for non-user based authentication, e.g. between *Retrieval Managers*).

Authorization: Permission, granted by a properly appointed person or persons, to perform some action.

Confidentiality: The protection of information from disclosure to those not intended to receive it.

Data Integrity: The assurance that data received is the same as data generated.

Domain: A system or portion of a system which has the same security policies and requirements. Individual agencies determine the boundaries of domains.

Non-repudiation: The ability of the receiver to prove that the sender of some data or of a request did in fact send the data even though the sender might later desire to deny ever having sent that data.

Proxy: A software agent that acts on behalf of a user.

Registration: The process whereby an individual submits required personal information to an agency and, in return, the agency provides the means (e.g. login name and password) necessary to perform authentication with the agency's system.

6.2 ICS Secure System Design

The ICS security controls are divided into three groups: administrative, physical and computing.

- Administrative security controls are policies, guidelines, and practices and procedures designed to manage and implement security.
- Physical security controls are physical barriers or devices designed to prevent harm to or loss of IT resources and assets, such as access control card readers, intrusion detection systems, and fire suppression systems.
- Computing security controls (sometimes called technical security controls) are software mechanisms designed to prevent harm to or loss of data and information.

Table 6-1 maps the vulnerability categories, discussed above, against the security control categories. The remaining sections in this chapter describe the specific security controls in each control category of administrative, physical and computing.

Table 6-1. ICS Vulnerabilities versus Security Controls

Vulnerabilities	Security Control Category		
	Administrative	**Physical**	**Computing**
Software Vulnerabilities.	CEOS ICS Software CM ICS Event handling Security Testing	Site facility protections*	Standards on RM development Fault Handling
Hardware Vulnerabilities.	Site hardware administration*	Site facility protections*	RM Response to Unavailability of Remote RM
Data Vulnerabilities.	RMA back up procedures Authentication Information Management	Physical security of hardware*	Access control - users Access control - RMA RM DBMS data integrity functions Time Out Features Tamper Proofing Encryption
Administrative Vulnerabilities.	Collection Manual ICS Administration Manual RMA Training ICS Event handling System Rules for Users CEOS Authorization		RM Administration Independence Display System Rules for Users RM Activity Logs
Communication Vulnerabilities.		Site disaster prevention Physical security of hardware*	Network security
Personnel Vulnerabilities.	RMA Training Site personnel practices*		RM Administration Independence
Facility Vulnerabilities.		Site physical security* Site maintenance*	

* Site security controls are assumed to be in place for the sites where *Retrieval Managers* will be installed.

6.2.1 Administrative Security Controls

Administrative security controls include security policy, and other items and activities that are designed to manage and implement security policy. They should provide security guidance to users and RMAs who have some level of authorization to use or have access to ICS resources. This section defines the security controls which are listed in the Administrative Security Column of Table 6-1.

CEOS ICS Software CM. To support the establishment of *Retrieval Managers,* ICS software will be made available for reuse. This will be accomplished using a configuration controlled access point for the distribution of ICS software. Configuration management, from a security point of view, provides assurance that the software which is available is the correct version (configuration) and that any changes to be made are reviewed for security implications. Configuration management can be used to help ensure that changes take place in an identifiable and controlled environment and that they do not unintentionally harm any of the system's properties, including security. Changes to the software can have security implications because they may introduce or remove vulnerabilities. Once an organization pulls code from an ICS reuse library, the ICS CM is longer in effect. It is possible for an organization to cause unintended erroneous action in ICS reuse code by modification outside of ICS. This will not threaten ICS due to the domain independence of the ICS elements, e.g., access to one *Retrieval Manager* does not automatically provide access to all Retrieval Managers.

ICS Event handling. Because the ICS operations depends on the loosely associated RMAs, procedures for dealing with events in the ICS are defined in advance. ICS events include: adding a new *Retrieval Manager*, alerting ICS to detection of an intrusion at a *Retrieval Manager*, alert of a *Retrieval Manager* being off-line either due to a planned or unplanned cause. The main communication amongst RMAs will be via an RMA e-mail list. Although for security alerts, communications must be by a separate channel than e-mail, e.g., phone, as an e-mail alert may be intercepted. The procedures for ICS event handling will be detailed in the ICS Administration Manual

Security Testing. Security testing is conducted to ensure that the security features meet technical specifications and to locate vulnerabilities. Examples of security testing tools are: Security Administrator Tool for Analyzing Networks (SATAN) and Internet Scanner, a product of Internet Security Systems, Inc. (ISS). These tools are designed to discover weaknesses or holes in a UNIX based network and recommend fixes. Procedures for ICS security testing will be detailed in the ICS Administration Manual

RMA Training In order to insure consistent ICS operations and adherence to procedures with security implications, ICS Training will be conducted for ICS RMAs. This training will cover, at a minimum, the material in the ICS Administration Manual.

System Rules for Users ICS users cannot be expected to act responsibly with respect to ICS operations, unless they are aware of the system rules for users. These rules should clearly delineate responsibilities of and expectations for all individuals with access to the system. Often rules should reflect logical security controls in the system. For example, rules regarding authentication should be consistent with technical features in the system.

Management Authorization The authorization of a system to process information, granted by a management official, provides an important quality control. By authorizing processing in a system, a manager accepts the risk associated with it. Management authorization should be based on an assessment of management, operational, and technical controls. Since the SDD establishes the security controls, it should form the basis for management authorization, supplemented by more specific studies as needed. In addition, periodic review of controls should also contribute to future authorizations. Re-authorization should occur prior to a significant change in processing, but at least every three years. It is important to

identify the appropriate management authorization for ICS. ICS is a CEOS activity and has the context defined by its interfaces (see ICS Context Diagram in Section 3). For ICS, the authorization must come from both the appropriate CEOS organization as well as individually by the agencies which host *Retrieval Managers*. The ICS is planned and authorized by the Access Sub-Group. Each agency operating a *Retrieval Manager* is represented in the Access Sub-Group.

6.2.2 Physical Security Control

Physical security controls are designed to guard against threats that result from both natural disaster (e.g., storms and resulting power outages) and human activity (e.g., fire, theft of hardware and software, physical access to a facility by unauthorized persons). All physical security controls listed in Table 6-1 are the responsibility of the sites which host a *Retrieval Manager* and therefore are not under the control of the ICS SDD.

ICS as a system is robust to a failure of physical security control at a single site, i.e., a security failure due to physical controls may cause a loss at the site but cannot result in a loss at another ICS site. Each *Retrieval Manager* is independent from a security authentication perspective such that the integrity of data is not threaten by a lapse in physical security at another site. From availability consideration, the loss of a particular *Retrieval Manager* could cause disruptions in the operations of ICS. The event handling measures described in Section 6.2.1 and the System Management in Section 7, provide for the response procedures which would be initiated in case of a *Retrieval Manager* failure due to a lapse in physical security control.

6.2.3 Computing Security Controls

A summary of Computing Security Controls is provided in the first part of this section. The remainder of the section describes the authentication in ICS and the Group Security Model.

6.2.3.1 Summary of Computing Security Controls

Computing security controls are software and firmware mechanisms used to limit access, detect intrusion, detect malicious logic and prevent its propagation, etc. This section defines the computing controls which are listed in the Computing Security Column of Table 6-1.

The following Computing Security Controls are required to be implemented in the *Retrieval Manager* based on requirements in the ICS URD [R2], Sections 3.1.2 and 3.2:

- Standards on *Retrieval Manager* software development
- *Retrieval Manager* Fault Handling
- Access Control (See also SDD, Section 6.2.3.2)
- *Retrieval Manager* DBMS data integrity functions
- Session Time Out control
- RM Administration Independence

The following Computing Security Controls are required to meet the ICS security design. Requirements will need to be added to the ICS URD [R2] to insure the ICS elements are compatible:

- *Retrieval Manager* Response to Unavailability of a Remote *Retrieval Manager*
- Display System Rules for Users

It is important to note that Network Security is covered as a CEOS Network Sub-Group topic. Network security covers the issues outside of the application level *Retrieval Manager* Security functions, e.g., IP address blocking in a communication router.

6.2.3.2 Authentication Mechanism

This section describes several topics which introduce the ICS design for authentication. First the two mechanisms provided by CIP are described, then two scenarios are described for a *target* authenticating an *origin.* This section address the application layer provision for authentication which CIP provides. It is also important to note that *Retrieval Managers* make use of IP address as a basic authentication of other *Retrieval Managers*.

To meet the ICS security requirements in the ICS URD [R2], a comprehensive approach to network security based on a well developed cryptographic mechanism is needed. Authentication occurs in the context of a *CIP Session.* A *CIP session* is composed of multiple CIP *operations*. A CIP *operation* consists of several messages. A CIP session is begun with an *initializeRequest* and ends with a *close*. The authentication protocol described below allows authenticated sessions as well as authentication for any specific operation.

Two mechanisms are provided in CIP for authentication: symmetric key and asymmetric key. In the symmetric. In the symmetric case, both the *target* and the *origin* are holding the same key, e.g., a username/password. In the asymmetric case, the *origin* and *target* are holding different but related keys, e.g., the *origin* holds a private key and the *target* holds a public key. Both approaches use a digital signature as the means to authenticate the *origin.* The digital signature contains information which could have only been constructed with the user's key.

In ICS, the symmetric key approach is the default approach for authentication. If a *Retrieval Manager* provides authentication, the symmetric approach must be provided. To provide for an agency's specific needs, a *Retrieval Manager* may choose to provide asymmetric key authentication. This approach is driven by the need to comply with laws regarding export of encryption algorithms.

The basic element of the symmetric key approach is a Message Authentication Code (MAC). A MAC is a key-dependent, one-way hash function, i.e., a secret, shared key is required to form the hash and the hash cannot be decoded. Only someone with the identical key can verify the hash by performing the same hash operation and verifying the result is identical. MACs are useful to provide authentication without privacy. The protocol does not use privacy as a basis, i.e., encryption is not used. The MAC for CIP is calculated using an MD5 hash. The MAC approach relies on a shared key between the *origin* and *target*. In this protocol the secret, shared key is a username/password which is particular to the user. How the *target* got the username/password is addressed in Section 7.

The asymmetric key approach is based on a set of related key pairs (public, private) used for the encryption and decryption of messages. A "digital signature" is obtained by encrypting a message hash combined with a timestamp with a private key. Such a message can be authenticated by a decryption based on the corresponding public key. In the CIP context, a client holds the private key and a Retrieval Manager holds (or has access to via a Certification Authority) the corresponding public key.

Use of CIP for authentication is shown below in two scenarios. The first scenario shows use of part of the protocol for authentication for a specific operation. The second scenario shows how an authenticated session is established during initialization of the session.

6.2.3.2.1 Authentication for an Operation

This section addresses how a user would be challenged for authentication credentials based on a request for a CIP service, e.g., placing an order. It is assumed that the user's session is not an authenticated session.

The messages for this authentication are shown in Figure 6-1. Specific contents of the messages are provided in the CIP Specification [R3].

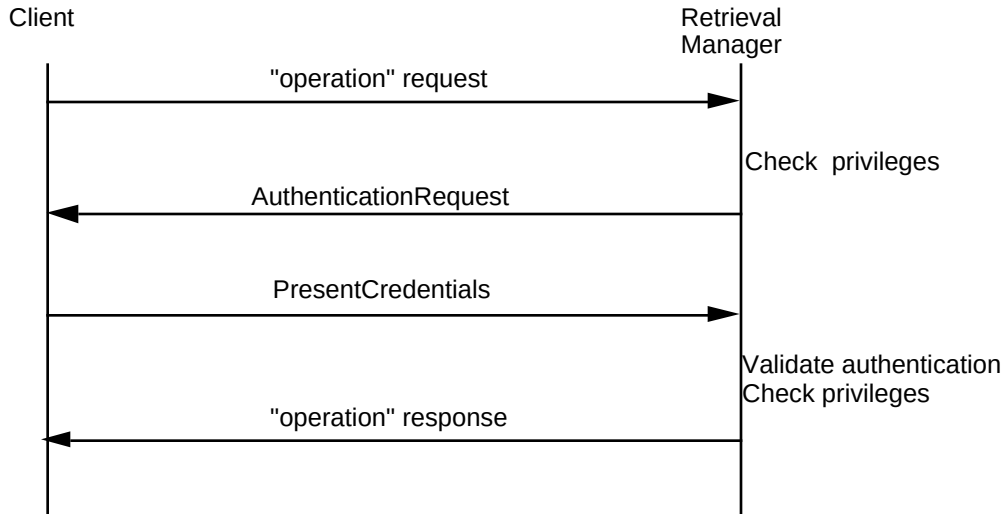

Figure 6-1. Authentication for an Operation

If Non-Repudiation is requested by the *Retrieval Manager*, another pair of messages would be needed in between *presentCredentials* and "operation" response. The first message would be from the *Retrieval Manager* to request a non-repudiated order from the client. The Client would reply with a non-repudiatable order message.

6.2.3.2.2 Authentication for a Session

This section addresses how a user would begin a session with the intent to have an authenticated session. The authentication is a two step process. First there is a two step authentication followed by a negotiation of cryptographic options including use of a session key.

The messages for this authentication are shown in Figure 6-2. Specific contents of the messages are provided in the CIP Specification [R3].

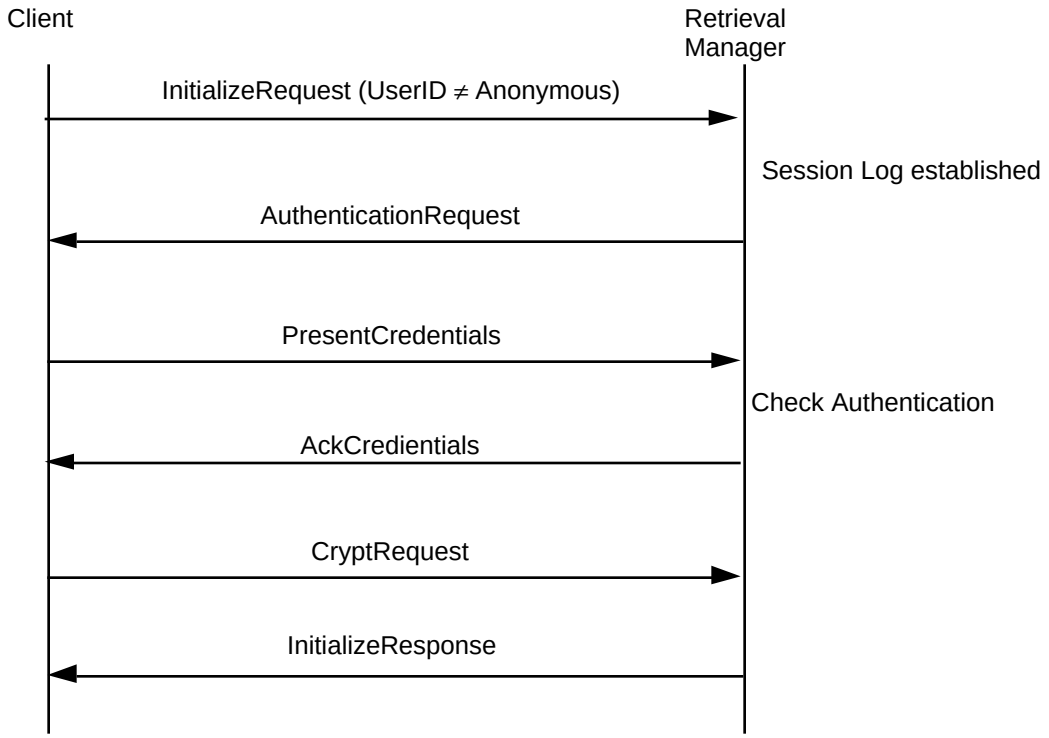

Figure 6-2. Authentication for a Session

6.2.3.3 Group Security Model

When security is considered in ICS - a distributed information system - the proliferation of credentials must be considered. The ICS has been designed to prevent a world-wide proliferation of usernames/passwords. The approach is to have the *Retrieval Managers* act as brokers for the users which they support. This avoids the user needing to be known at each *Retrieval Manager*. The *Retrieval Managers* serve as brokers based on two relationships: 1) a *Retrieval Manager* will support many users and 2) a *Retrieval Manager* is known to other *Retrieval Managers.*

The group security approach applies to any distributed session. The approach is most important when applied to ordering as ordering will require the highest security considerations. Figure 6-3 shows the focusing of orders by a home *Retrieval Manager*. "Home" in this case means that the user is registered at the *Retrieval Manager,* and for this example the user belongs to a group that has privileges to allow the order. Figure 6-3 shows multiple users sending order messages to the home *Retrieval Manager*. The home *Retrieval Manager* in turn, creates a secondary order message to the remote *Retrieval Manager* which holds the data. Each primary order from a user results in a secondary order between *Retrieval Managers*. The secondary orders are allowed based on the authentication between *Retrieval Managers* and the group membership of the local *Retrieval Manager*. The home *Retrieval Manager* maintains a cross reference of the primary order with the secondary order which was submitted to the remote *Retrieval Manager*.

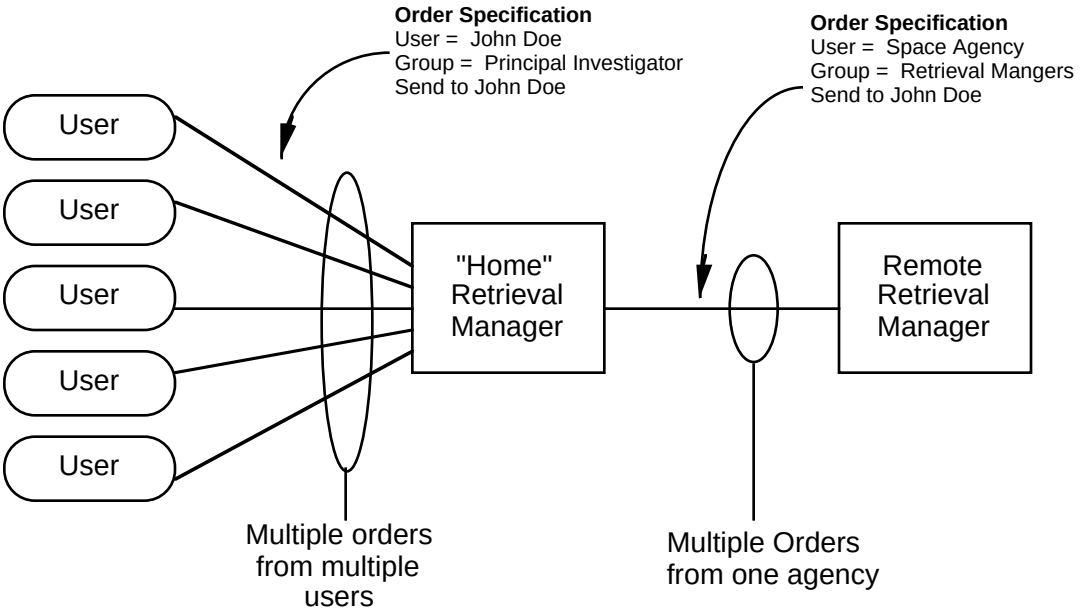

Figure 6-3. Group Ordering Model

The ordering described in Figure 6-3 and the associated text is the Order by Proxy approach. That is the *Retrieval Manager* is acting as the user's proxy to order the data on the users behalf. In the Order by Proxy case there is an agreement between agencies whereby one agency guarantees payment to another agency.

ICS also allows a second case labeled the Passthrough case. In the Passthrough Case there is a mechanism in the CIP to allow pass-through of information needed by an agency to perform its own authentication and authorization. There may be cases where agreements outlined in the Order by Proxy Case cannot be reached between agencies. Passthrough is a different method for ordering data that will provide convenience to the user. If a user who has a session established with the local *Retrieval Manager* (in Figure 6-3) wishes to order data from the Remote *Retrieval Manager* and is registered with a remote *Retrieval Manager*, the CIP can pass information (e.g. username/password) in a secure manner through the local *Retrieval Manager* to the remote *Retrieval Manager*. The remote *Retrieval Manager* then performs authentication and authorization for the user.

6.2.3.4 Group Management

Access control in ICS will be done according to the user's membership in a group. Privileges for access requests will be assigned to groups. Users will be associated with a group for a specific session. Administration of the groups and group privileges is discussed in this section.

For system management purposes, several groups will be defined for the whole of ICS. Use of these names will not be mandatory, but the group names shall be reserved and use of the ICS groups will be highly recommended.

The group to which a user belongs determines which data and services a user has access to, what the price will be, and whether the user is authorized to make the purchase (i.e. has sufficient money or credit limit). Order functions such as Order Quote and Submit Order require user information.

The following are examples of groups that may be used to determine authorization and associated services that would be made available to the user.

Table 6-2. ICS Groups and Privileges

Group Name	Group Privileges
Guest	- log on and log off - issue a collection search at any CIP target - retrieve collection search results from CIP targets - utilize a CIP target's Guide service
ICS Browse User	Guest privileges plus retrieval of browse data
ICS Order User	ICS Browse User privileges plus functions related to order CEOS data. (Note that this group will nominally have the privilege to order data for which there is no charge, additional privileges are needed to order data which requires billing and accounting.)

Agencies must have a policy regarding user access to ICS. This is especially true in the Proxy Case of the user model where the user's agency is taking responsibility for the charges incurred by the user at another agency. The following points determine a user's access privileges to the CIP:

1. The User's Agency will perform authentication on the User.
2. The User's Agency will manage the User's access and privileges.
3. If the User is registered, the registration will be with the User's Agency.
4. *Retrieval Managers* may use group designations to prioritize user access to CIP *Retrieval Managers* for resource control and system load throttling.

For Indirect Ordering (See section 3.5), the user wants to order from a remote *Retrieval Manager*. In this case the *Retrieval Manager* at the User's Agency acts as the intermediary *Retrieval Manager*. The following points determine a user's access privileges to the Remote *Retrieval Manager*:

1. The Remote Agency is responsible for authentication of users on an individual basis.
2. The Remote Agency is responsible for determining group designations for users.
3. The Remote Agency may use the Intermediary Agency's group designation to prioritize access to the Remote *Retrieval Manager* for resource control and system load throttling.

7. SYSTEM MANAGEMENT VIEW

This section discusses the Systems Management view of ICS. This view includes operational elements needed for monitoring, diagnosing and correcting operational elements of ICS.

System Management is a priority for ICS Release C. The remainder of the material in this section is a list of topics which need to be developed for Release C.

ICS System Management is the management of the ICS federation for issues such as security, networks, and distributed collection maintenance. All of these tasks must be defined in a distributed fashion to support the ICS Federation.

CEOS ICS Software CM. How will ICS shareware, e.g. *Retrieval Manager*, be made available? Need to insure that code cannot be modified and placed back on the server without a review process.

ICS Testing. The only specific testing addressed in the SDD is security testing. Certainly there will be integration and full-up system testing, perhaps a regression test after a new *Retrieval Manager* is added.

CIP Attribute Management. The ICS URD discusses several ways in which CIP attributes will be maintained and changed as the system is used. It is not clear who will have the responsibility for the various ways in which attributes will evolve.

ICS Event Handling. Procedures for dealing with events in the ICS. Events include adding a new RM, alert to detection of an intrusion to an RM, alert to RM down, e.g. for maintenance. Includes use of an RMA e-mailing List.

ICS Monitoring Center. Although the System Management approach is for each ICS site to manage its site, there may be a need for one site to be tasked with monitoring the system as a whole and coordinating system wide responses.

Security Information Management. Practice for management of authentication information, e.g. passwords. Practice for management of authorization information, e.g. group privileges. Management groups definition common across retrieval managers.

Statistics Collection. Each retrieval manager will be collecting statistics on ICS usage. There will be value in standardizing statistics reports to support sharing of information.

CEOS Network Management. SDD discusses need for network management. This will need to be coordinated with the CEOS Network Sub-group.

ICS Administration Manual. Need to develop an ICS Administration Manual for RMAs to use. It would include how to configure RM software, security information management, agency-to-agency billing, event handling procedures, etc.

RMA Training. CEOS organized training for RMAs based on the ICS Administration Manual

RMA Mailing List. An e-mail mailing list with all RMAs subscribed. Message types to RMA Mailing List: alerts, statistics, RMA lessons learned or hints.

Development of this section should consider the following sources:

- CINTEX Lessons Learned.
- CINTEX Federation Management paper.
- Member Agency Control Authority Office (MACAO) procedures for SFDU management as defined by CCSDS Panel 2 (see the following for more information: http://bolero.gsfc.nasa.gov/ccsds)
- NASA ECS System Monitoring and Control center design and operations approach.

8. ARCHITECTURE VERIFICATION

This chapter provides the results of several types of analysis which demonstrate that the system design described in the previous chapters will meet the ICS requirements and that the various architectural views are consistent. The analysis results in this chapter also provide design information for the developers of the particular elements of the ICS.

8.1 Scenarios

This section provides several scenarios showing the dynamic aspects of the ICS including how the scenarios are accomplished via interfaces between ICS elements and services of the ICS elements. Scenarios for both the user's and operator's activities are provided.

Scenarios in this section are organized into the following categories:

- User Scenarios
  - WWW Access to a *Retrieval Manager*
  - Existing Agency Client Access into ICS
  - Indirect Ordering Scenario
- Collection Population Scenarios
  - Making a CIP Compatible Catalogue Available
  - Collection Established for an Event
- System Management Scenarios

8.1.1 User Scenarios

8.1.1.1 WWW Access to a *Retrieval Manager*

8.1.1.1.1 General

The scope of this scenario is to follow a user's confrontation with the system and to simulate whether a user can successfully retrieve helpful documents and EO-data from the ICS and related Catalogues.

This scenario is based on the CEO Enabling Services Scenario 1: Search for EO-data, documents and adverts [R17]

8.1.1.1.2 Assumptions

- The user is familiar with WWW browsers, has access to a web browser, is connected to the Internet and knows the HTTP address of a CIP/WWW Gateway.
- He has only a basic knowledge of remote sensing.

- The user works for a consultancy company that is specialized in identifying and evaluating potential water reservoirs in third world countries.
- The present project aims to build a water reservoir in Egypt. He has an explicit question he needs to be answered: Is a high resolution elevation model of this area available?
- He is interested in any documents related to this subject.
- The user has never entered the ICS before and is therefore not registered. The scenario does not include an authorization operation and the user is considered a member of the "guest" group.

8.1.1.1.3 Expected Outputs

The user wants to find out if a DEM of the target region is available. For the DEM data he hopes to find explicit meta-data that describes the data (i.e. browse) before he orders it. (He tries finding documents covering this subject.)

8.1.1.1.4 Step Sequence

1. The user enters the CIP/WWW Gateway home page for a *Retrieval Manager*.
2. He reads the short introduction about what the local *Retrieval Manager* can do for him.
3. He enters the "EO-data search" interface. The user has the choice between a local or remote collection search , a data search against the entire ICS holdings (using the global node) , a local search against the entire local site holdings (using the root node), or against popular topics (using the key access nodes).
4. The user chooses the local collection search of the root collection after reading the short definition supplied by the system. The form that is supplied contains fields in which the search attributes have to be entered.
5. The user selects DEM from the listed "product attributes".
6. He selects "display full valid definition" to make sure the acronym is he expected.
7. The system displays the full definition of a digital elevation model.
8. The definition is what the user expected and the user submits the local collection search.
9. After a syntax check of the search the system accepts the search.
10. The system returns a structured list of collections which point to data that incorporates DEMs. One of the listed collections is called: "Elevation Models of Africa; ESA; 1992".
11. The user chooses: continue with "EO- product search".
12. The system displays a form which contains attribute fields.
13. The user chooses the: "Elevation Model of Africa; ESA; 1992" and another elevation model terminal collections from the collection list. (The collection may be chosen in the collection search).
14. The user chooses the "select geographical region" option.
15. This gives him the following choices:
    - type global coordinates
    - draw area of interest by polygon

- draw area of interest by point and radius

16. The user chooses “type global coordinate”.
17. He enters the coordinates for Egypt.
18. He submits the EO-product search.
19. The system indicates that the search is valid after a successful syntax check has been performed.
20. (Note this step was deleted from the CEO scenario as CEOS policy is to not charge for searching.)
21. The user asks for a “status monitor” to display the status of the search.
22. A status monitor is displayed showing the two parallel searches (compare to step 13). The search “Elevation Models of Africa, ESA, 1992” is finished but the second search has not received any reply by the provider site yet.
23. The user selects “display product list”.
24. The results of the EO product searches are displayed in a list.
25. The information displayed contains information on the location, provider, title and the availability of on-line meta-data and browse data.
26. The user selects a product.
27. The user chooses the “transfer metadata” option.
28. The metadata is transferred and displayed.
29. The user chooses the “transfer browse product” option.
30. The browse product is transferred and displayed.
31. The user selects the “order product” option and orders the product delivered via ftp.
32. An FTP-session is started and the product is transferred to the machine of the user. *Steps 32 and 33 are outside the ICS, but they are mentioned here for completeness purposes*.
33. The user saves this file on his hard disk.
34. The user chooses the “save EO-data search” option.
35. The system saves the “data search ” (the system stores this internally while this session continues).
36. The user chooses the “save EO-data search results” option. (The result set is converted to a hot collection, held on the users client.)
37. The system saves the “EO-data search results”.

8.1.1.2 Existing Agency Client Access into ICS

8.1.1.2.1 General

This scenario follows both the user steps and the system software steps for an agency's user to access and order products held in the ICS collections using his local client software and an ICS gateway. The scenario concentrates on the user visible processes and the interaction between the *ICS Gateway* and the ICS *Retrieval Managers*.

8.1.1.2.2 Assumptions

1. User is an experienced, registered User of his local Agency (Agency A) catalogue system and is using his local Client.

2. Agency A has 2 way interoperability with ICS that is transparent to the users of its systems.

3. The User has established a session with his local catalogue systems as a registered user

4. The user is interested in AVHRR data over Europe (resident in ESA ICS holdings)

5. The user has no ICS experience and is not a registered user

6. The local agency catalogue system has been configured to recognize ICS collections through a catalog/Gateway configuration

7. Agency A and ESA have a trust agreement for authentication.

8. ESA and Agency A have a bilateral agreement that allows Agency A to act as a proxy for its users to order data. ESA bills Agency A for data ordered by its users.

9. The scenario assumes the ICS Functional Framework shown in Figure 3-3.

Agency A architecture is similar to third site in Figure 3-9 i.e., *Retrieval Manager* as a catalogue gateway.

8.1.1.2.3 Expected Outputs

The user uses his local client (*Existing Agency Client)* and finds new data through the *Retrieval Manager* which is held at a site to which his site previously did not have access.

8.1.1.2.4 Scenario Sequence

SEARCH SUB SCENARIO

1. Human user initiates local catalogue system client and logs in as a registered user

2. The user develops a query to discover any products containing AVHRR data over Rome taken in the 1995-1997 time frame.

3. Based on the contents of the query and information from the local agency catalogue the query is sent to the ICS Gateway

4. *ICS Gateway* translates the query from the local query language (e.g., ESQL) to the CIP Query format (RPN) and translates local agency attribute names attributes into appropriate CIP attributes

5. *ICS Gateway* interacts with the local catalogue system to determine which ICS sites can satisfy the query

6. The *ICS Gateway* acts as a ICS *CIP Client* and establishes a session to the Agency A *Retrieval Manager* (RM) using CIP and sends the query to the Agency A RM

7. The RM then sends the query to the remote *Retrieval Managers* which pose queries to local collections and return results to the local agency ICS Gateway.

8. The *ICS Gateway* translates the returned result set into local format and returns the result set to the Client.

9. The human user evaluates the results and requests browse attributes for four data products of interest in ESA collections

10. Steps 3-8 repeated

11. The user decides to order the four products

ORDER SUB SCENARIO

12. The local Client puts up an order specification form which the user fills out

13. The local Client sends an order quote request to the ICS Gateway

14. The *ICS Gateway* translates the order quote message into CIP format and the local product identifiers into appropriate CIP product identifiers

15. The *ICS Gateway* acts as a *CIP Client* and establishes a session to the Agency A *Retrieval Manager* (RM) using CIP and sends the quote request to the Agency A RM

16. The Agency A RM sets up an authenticated session with the ESA RM as Agency A via the CIP to obtain Agency A session options.

17. The Agency A RM sends the quote request to the ESA RM and requests a price estimate for the order.

18. The ESA RM forwards the quote request to the local Order Handling System (OHS) which returns the estimate to the ESA RM.

19. The ESA RM returns the quote to Agency A RM.

20. The Agency A RM forwards the estimate to the ICS Gateway

21. The *ICS Gateway* translates the returned message into local format and returns the message to the Client

22. The user reviews the estimate and requests the order be submitted

23. The *ICS Gateway* checks the user's credit via an interaction with the Agency A Billing and Credit Subsystem and on credit approval obtains an order number for local billing

24. The *ICS Gateway* translates the estimate approval format into CIP and forwards it to the Agency A RM which forwards it to the ESA RM which forwards it to the local OHS

25. The local OHS accepts the order and sends a status update of Order Acceptance to the ESA RM which forwards it to the Agency A RM which forwards it to the ICS Gateway

26. The *ICS Gateway* translates the message to the Agency A format and order number and informs the local Client and the local Billing and Credit subsystem of the order status

27. The human user logs off his local client and all sessions are terminated

8.1.1.3 Indirect Ordering Scenario

8.1.1.3.1 General

The scope of this scenario is to show how a user places an order with a *Retrieval Manager* at which he is registered (*Retrieval Manager* - A) and, transparent to the user, the order is routed to another *Retrieval Manager* (*Retrieval Manager* - B) which has access to the products.

8.1.1.3.2 Assumptions

1. User has performed a search process and obtained the identifiers of a set of products which he wishes to order.
2. The user's agency and the data holding agency have an agreement that allows the user's agency to act as a proxy for its users to order data. The data holding agency will bill the user's agency for the data. The user's agency will bill the user for the data.
3. The order is placed with a *Retrieval Manager* (*Retrieval Manager* - A) with which the user is registered and has privileges sufficient to allow the order.
4. The Intermediary *Retrieval Manager* (*Retrieval Manager* - A) is authenticated with the *Retrieval Manager* which will fill the order (*Retrieval Manager* - B).
5. The order will be delivered in media, e.g. CD-ROM.
6. The user has established an authenticated session with *Retrieval Manager* - A.
7. *Retrieval Manager* - A has established and authenticated session with *Retrieval Manager* - B.

8.1.1.3.3 Expected Outputs

The user reviews a quote for the order, submits the order, and receives the products some time later.

8.1.1.3.4 Step Sequence

1. The *CIP Client* displays an order form which the user fills out.
2. User chooses to be charged by his own agency (not the agency that holds the data).
3. The *CIP Client* sends the order request to *Retrieval Manager* - A as part of an authenticated session.
4. *Retrieval Manager* - A determines the user's privileges based upon the user's group membership for that session. The group privileges allow this order request.
5. *Retrieval Manager* - A identifies the site from which data is being ordered (*Retrieval Manager* - B) based on information in the product identifiers in the order.
6. *Retrieval Manager* - A sends the order request and a group designation to *Retrieval Manager* - B as part of an authenticated session. (Note that the group designation in this session is for the *Retrieval Manager* - A session and may differ from the group of the client's session.)
7. *Retrieval Manager* - B determines the privileges based upon group membership. The group privileges allow this order.
8. *Retrieval Manager* - B forwards the order to the *OHS Translator* which converts the order into a local OHS order. The translator then passes the order to the OHS.

9. The OHS produces a quote and cost breakdown and assigns a quote number.

10. OHS sends quote, cost breakdown and quote number to *Retrieval Manager* - B (via the *OHS Translator*) which forwards it to *Retrieval Manager* - A which forwards it to the *CIP Client*.

[Steps 2-10 can be repeated by the user by changing and re-submitting the order specification to get data pricing information.]

11. The user reviews the quote and decides to submit the order. The *CIP Client* sends the order submittal to *Retrieval Manager* - A.

12. The group privileges for the user's session allow this order but determines that the order must be non-repudiatable. *Retrieval Manager* - A sends a non-repudiation request to the CIP Client

13. The *CIP Client* requests the user to confirm the order submittal, which the user does.

14. The *CIP Client* sends the order as a non-repudiatable message to *Retrieval Manager* - A.

15. *Retrieval Manager* - A sends order submittal to *Retrieval Manager* - B.

16. *Retrieval Manager* - B determines the group privileges associated with the session with *Retrieval Manager* - A and allows the order submittal.

17. *Retrieval Manager* - B passes the order submittal to the local *OHS* (via the *OHS Translator*).

18. OHS accepts the order, determines an expected order completion date, and returns an order submittal response to *Retrieval Manager* - B.

19. *Retrieval Manager* - B passes the order submittal response to *Retrieval Manager* - A.

20. *Retrieval Manager* - A notifies the local *OHS* (via the *OHS Translator*) that the order submittal has been accepted.

21. The OHS associated with *Retrieval Manager*-A does the accounting and billing associated with the order and the user's account.

22. *Retrieval Manager* - A passes the order submittal response to the CIP Client.

23. Possibly after the users session is closed, the OHS associated with *Retrieval Manager* - B fills the order and sends the bill to the OHS associated with *Retrieval Manager* - A.

8.1.2 Collection Population Scenarios

This section contains scenarios concerning establishment of collections.

- Establishing collections in a *Retrieval Manager* for the first time
- Creating a new Provider Theme collection in response to a Earth Science Event

8.1.2.1 Making a CIP Compatible Catalogue Available

8.1.2.1.1 General

A provider who works for a large company wants to make his scanned aerial pictures accessible through the ICS.

This scenario is roughly based on CEO-ES Scenario 4: Making a CIP compliant catalogue available.

8.1.2.1.2 Assumptions

The following assumptions apply to this scenario:

- The provider has an Internet connection and a UNIX workstation.
- The provider has an existing inventory system on a relational database system which catalogues all the data products archived at the company.
- The catalogue the provider wants to make available is an EO-data catalogue.

8.1.2.1.3 Expected Outputs

The catalogue of the provider becomes accessible for the ES users.

8.1.2.1.4 Step Sequence

1. The potential data provider attends a CEOS meeting and decides to host a *Retrieval Manager*
2. Reviews CEOS documentation describing ICS
3. Accesses the CEOS *Retrieval Manager* software distribution site
4. Retrieves RM source code
5. Configures the *Retrieval Manager* for his specific environment
6. Develops translator for local inventory searches reusing a skeleton *Catalogue Translator*.
7. Develops a gateway from the RM to his local Order Handling System (OHS) by reusing the local OHS provided with the RM
8. Establishes Provider Archive Collections for each of his existing datasets by developing Collection Descriptors for each of the datasets and an Explain database which lists the available services at his RM, and describes some product specific attributes which are used in the local catalogue systems to describe specific details of the individual photographs
9. Establishes a Provider Theme Collection which combines several existing datasets which contain aerial photographs and modifies the Explain Database to list the new Provider Theme Collection as a Key Access node
10. Establishes a root collection that references all the collections at the local site
11. Contacts the Global Collection *Retrieval Manager* Administrator (*RMA*) via email and describes the datasets that have been established. The Global Collection *RMA* advises the provider as to the keyword that should be used to characterize his collections and some remote collections that have similar themes
12. The provider modifies his root collection and his Provider collection to reflect the discussions with the Global Collection *RMA*
13. Conducts local test of *Retrieval Manager* and collections
14. Send a message to the Global Collection *RMA* announcing his desire to bring up a *Retrieval Manager* and join the ICS and puts the RM on-line to allow remote testing
15. The Global Collection *RMA* performs integration testing on the new provider site, and when he is satisfied at the results, adds the root collection of the new provider site to the global collection and

announces the availability of the new provider site and collections to the ICS community via email and the WWW.

16. The *RMA* at the new site continues to evolve his collections by adding new Provider Theme Archives and adding references to remote collections of interest to each of his collections

8.1.2.2 Collection Established for an Event

8.1.2.2.1 General

This scenario demonstrates how a Provider Theme Collection is created. The scenario shows the interaction of the *RMA* and a scientist for the creation of the collection. The collection is created based on an event of particular weather patterns over the Andes.

This scenario is based on a scenario titled 'Climate, Erosion, and Tectonics in the Andes and other Mountain Systems,' which is ECS Scenario 22B, in [R22].

8.1.2.2.2 Assumptions

The following assumptions apply to this scenario:

- The user is a scientist at an agency which hosts a RM
- The user has discovered an interesting event analyzing data from an instrument.

8.1.2.2.3 Expected Outputs

The user wants to establish a collection for the event which his colleagues may access.

8.1.2.2.4 Step Sequence

1. A severe storm in the Andes is detected by user's review of MODIS Level 2 Imagery Products
2. User searches in ICS for other data products which overlap the event in temporal and spatial location.
3. The user establishes a hot collection based on the result set returned from his query. this results set contains data granules from MODIS, MISR, ASTER, GLAS, LANDSAT-7, ERS-2, ADEOS, and RADARSAT.
4. The user conducts incremental queries on the hot collection holdings to narrow the collection by determining the quality of each product and the degree of overlap with the storm track
5. The user establishes the final refined result set as a hot collection and deletes the earlier established hot collection
6. The user orders all the products remaining in his hot collection and applies various analysis techniques to detect the presence of the event in the other sensor data
7. The user uses hot collection editing tools to eliminate the products that do not show effects(e.g. landslides or floods) from the storm and contacts his local site *RMA* to request his hot collection be upgraded to a User Theme Collection.
8. The user writes a paper on the event and lists the URL for the collection requesting reviews by his colleagues to verify and augment his conclusions

9. The user receives several favorable reviews of his research and contacts his local *RMA* about the possibility of having the agency publicize and maintain the collection for long term preservation
10. The *RMA* and the agency science review board reviews the collection and the colleague comments and agrees to ingest the collection into the agency archive.
11. The *RMA* sends a form to the user requesting needed metadata about the collection. The user fills out the form and returns it to the *RMA*.
12. The *RMA* converts the user theme collection to a provider theme collection by upgrading the metadata, including the collection descriptor in the RM root collection.
13. The *RMA* advertises the collection via Email , bulletin boards and the CEO advertising service.
14. All ICS users are now able to access and search Andes Severe Weather Event Provider Theme Collection.

8.1.3 System Management Scenarios

This section will contain scenarios concerning ICS System Management. As System Management is an ICS Release C focus, these section contains short descriptions which may be developed for Release C.

Retrieval Manager Registration. The scope of this scenario is to show how a *Retrieval Manager* becomes registered as an ICS *Retrieval Manager* and subsequently supports authenticated *CIP sessions* to allow ordering.

Planning a Retrieval Manager Outage. The scope of this scenario is to show how the *RMA*s work as a distributed management team. It is assumed that *RMA*s are trained in ICS Systems Administration procedures, a certain *Retrieval Manager* has been operational for some time and is remotely linked by many other *Retrieval Managers*, and the *Retrieval Manager* must be down from operations for several hours to change a piece of hardware. The expected output is that disruptions to ICS users are minimal and any users calls to *RMAs* are handled in an informed manner.

Response to Retrieval Manager Fault Condition. The scope of this scenario is to demonstrate the use of the *Retrieval Manager* monitoring functions by an operator in abnormal situations. It should be noted that the problems encountered in this scenarios are not representative of the ICS normal behavior and are presented here for illustration purposes. This scenario is based on CEO-ES Scenario 8: Middleware node operator - Use of the monitoring server.

8.2 Internal Interface Identification

Interfaces for the various ICS components have been stated in the multiple architectural views provided in the previous sections of the SDD. This section provides a summary of the interfaces between ICS components insuring consistency and completeness.

8.2.1 Retrieval Manager Interfaces

The *Retrieval Manager* has the interfaces indicated in Table 8-1.

Table 8-1. Retrieval Manager Interfaces

Other ICS or Related Element	Interface	SDD Section
CIP Client Application	CIP sessions	3.5.1
CIP Client Application	CIP messages	4.7
CIP Client Application	Socket Connection per CIP Session	5.1.4
CIP Client Application	TCP/IP via National Internet	5.2.1
CIP Client Application	TCP/IP via World-wide Internet	5.2.1
Other z39.50 Clients	Z39.50, Version 3 sessions	3.5.1
Other z39.50 Clients	Subset of Z39.50, Version 3 data	4.7
Other *Retrieval Managers*	CIP sessions	3.5.1
Other *Retrieval Managers*	CIP messages	4.7
Other *Retrieval Managers*	Persistent Socket Connection	5.1.4
Other *Retrieval Managers*	TCP/IP via National Internet	5.2.1
Other *Retrieval Managers*	TCP/IP via World-wide Internet	5.2.1
Other *Retrieval Managers*	TCP/IP via CEOSnet	5.2.1
Catalogue Translator	CIP sessions	3.5.1
Catalogue Translator	Subset of CIP messages	4.7
OHS Translator	CIP sessions	3.5.1
OHS Translator	Subset of CIP messages	4.7
UPS Translator	UPS Session	3.5.1
UPS Translator	User Management Information	4.7
UPS Translator	Username/Passwords	6.2.3.2
RMA	Operator Interface	3.5.1
RMA	Operator Interface Data	4.7
RMA	Username/Passwords	6.2.3.2
Collection Management Tools	Collection Data Base Modification	3.5.1
Collection Management Tools	CMT Messages	4.7
Monitoring and Control Tools	*Retrieval Manager* Management	3.5.1
Monitoring and Control Tools	MCT Messages	4.7
TCP Application on *Retrieval Manager* Host	TCP/IP Services	5.1.3
Site Physical Facilities	Physical Security Control	6.2.2

8.2.2 CIP Client Application Interfaces

The *CIP Client* Application has the functional interfaces indicated in Table 8-2.

Table 8-2. CIP Client Application Interfaces

Other ICS or Related Element	Interface	SDD Section
Retrieval Manager	CIP sessions	3.5.2
Retrieval Manager	Socket Connection per CIP Session	5.1.4
Retrieval Manager	TCP/IP via National Internet	5.2.1
Retrieval Manager	TCP/IP via World-wide Internet	5.2.1
HTTP/CIP Gateway	CIP sessions	3.5.2
CIP Client Presentation Layer	Data to user	3.5.2
TCP Application on *CIP Client* Application Host	TCP/IP Services	5.1.3

8.2.3 Retrieval Manager Administrator (RMA) Interfaces

The *RMA* has the operational interfaces indicated in Table 8-3.

Table 8-3. Retrieval Manager Administrator Interfaces

Other ICS or Related Element	Interface	SDD Section
Retrieval Manager	Operator Interface	3.5.3
Retrieval Manager	Physical Security	6.2.2
Collection Management Tools	Operator Interface	3.5.3
Monitoring and Control Tools	Operator Interface	3.5.3
ICS User	Username/Password	6.2.3.2
Other *RMAs*	Inter-Agency Billing Agreements	6.2.3.3
Other *RMAs*	Inter-Agency Security Agreements	6.2.3.3
Other *RMAs*	Group Management	6.2.3.4
Other *RMAs*	System Administration	7.
Interfaces outside of ICS	*OHS Translator*, *UPS Translator*, *Catalogue Translator*, OHS, UPS, Catalogue, Archive.	3.5.3

8.2.4 Collection Management Tools (CMT) Interfaces

The CMT has the interfaces indicated in Table 8-4.

Table 8-4. Collection Management Tools Interfaces

Other ICS or Related Element	Interface	SDD Section
Retrieval Manager	Collection Data Base Modification	3.5.4
Retrieval Manager	CMT Messages	4.7
Retrieval Manager Administrator	Operator Interface	3.5.4
Interfaces outside of ICS	Data file ingest	3.5.4

8.2.5 Monitoring and Control Tools (MCT) Interfaces

The MCT has the interfaces indicated in Table 8-5.

Table 8-5. Monitoring and Control Tools Interfaces

Other ICS or Related Element	Interface	SDD Section
Retrieval Manager	*Retrieval Manager* Management	3.5.5
Retrieval Manager	MCT Messages	4.7
Retrieval Manager Administrator	Operator Interface	3.5.5
Interfaces outside of ICS	*OHS Translator*, *UPS Translator*, *Catalogue Translator*, OHS, UPS, Catalogue, Archive.	3.5.4

8.3 Query Performance Estimates

The development of Query performance estimates is detailed in the ICS Query Performance Study [R19], only a brief outline of the development is presented here. The estimates are provided here to allow design to proceed against an acceptable query performance baseline. Achieving distributed query performance which is acceptable to users is critical to the usability and success of ICS.

Search queries within ICS can be either against the local *Retrieval Manager* or distributed over various *Retrieval Managers* in the ICS. The data being queried may be either collection descriptors or product descriptors. These two divisions form four natural domains within which the query performance can be analyzed. These domains are: local collection searches, local product description searches, distributed collection searches, and distributed product description searches. Each of these are treated in subsequent subsections.

In the course of developing performance estimates several assumptions had to be made. These assumptions are listed below. It was also necessary to estimate a number of parameters. The parameters and their nominal values are listed in a subsequent subsection.

For distributed queries the collections have been modeled as a uniform tree (a type of directed graph). A specific definition of uniform trees may be found in the Collection Technical Note [R11]. Use of this approach allows estimations to be made of the probability that any particular *Retrieval Manager* will be the target of a subquery.

Query performance is highly dependent on how well the underlying database tables are laid out and how well the queries map into the database tables. This point is important enough that it was felt that it should be given the visibility of an assumption.

[A0] It is assumed that within a given *Retrieval Manager* the collection database has been well laid out and is fairly efficient with regard to the expected queries.

Related to this assumption is the feeling that all collections held by a single *Retrieval Manager* should be organized into single database. This is mentioned because the naive approach would be to treat each collection as if it were a separate database. This would lead to multiple subqueries on the same *Retrieval Manager* to accomplish the query.

[A1] The number of messages that will be passed between *Retrieval Managers* is proportional to the fraction of all collection–to–collection links that point to a collection held by another *Retrieval Manager*. This is the "R" parameter listed in Table 5-3. As an example, if all collections were local, the R parameter would be zero (0). Likewise, if every collection pointed to a collection held by another *Retrieval Manager*, the R parameter would be one (1).

[A2] The probability that a specific *Retrieval Manager* is referenced by another *Retrieval Manager* is uniform (all *Retrieval Managers* are equally likely to be referenced). The best way to determine which *Retrieval Manager* will be referenced is to examine the collections and count which *Retrieval Managers* are referenced most often. Since that is not possible at this stage, this assumption allows a way to determine how messages are routed.

[A3] For LAN networks, the network time, including time to form Z–associations, is small compared to the time required to service a query. We make this assumption because we would like to be able to ignore the physical connections of a local *Retrieval Manager*, any *Catalogue Translator*s associated with it, and the local catalogue system. If the time spent transferring information between these systems is small it is valid to ignore the interconnections.

[A4] *Retrieval Managers* and related elements (such as networks) involved in subqueries of a single query (or higher order subquery) will operate in parallel. An example of this is if a query being performed at *RMA* requires subqueries to be performed by RM_B and RM_C, *RMA* will send the subqueries to RM_B and RM_C simultaneously rather than sequentially. RM_B and RM_C will perform their subqueries in parallel and present their response to *RMA* basically simultaneously.

[A5] All elements (*Retrieval Managers*, networks, translators, etc.) can be modeled as M/M/1 queues. If this is not the case, as would be the case if some element had multiple servers, then certain equations in the distributed query cases may have to be revisited. (See [R21] for a discussion of Queuing Theory.)

8.3.1 Local Collection Searches

If the *Retrieval Manager* is modeled as a M/M/1 queue, it is fairly easy to show that the average time to perform a search of the local collections is given by:

$$t_{local,col} = d_{col} \Big/ (1 - \rho_{RM})$$

Since there are requirements specifying that the response time to a local query shall be less than 5 seconds on the average and since performance is to be measured under a 50% load, we can easily calculate that the service time required for a strictly local collections search must be 2.5 seconds or less.

8.3.2 Local Product Description Searches

The Local Product Search differs from the Local Collection Search in that it must step outside of the CIP domain. In order for the query (or subquery) to be a valid query for the inventory catalogue system, the query must pass through a *Catalogue Translator.* If we can ignore how the *Retrieval Manager*, Translator, and Catalogue systems are physically interconnected, we can calculate the average response to a local product description search:

$$t_{local,prod} = t_{local,col} + (1 - O_{col}) \times A^{depth/2} \times \left(d_{xlate} / (1 - \rho_{xlate}) + d_{inv} / (1 - \rho_{inv}) \right)$$

If the network time can not be neglected, then an additional term must be added to $t_{local,prod}$. This term will vary with the physical layout of the local site. Therefore a single form of the term can not be offered here. It will have to be determined in collaboration with the local site manager.

8.3.3 Distributed Collection Searches

In a distributed collection search, one or more of the collections held by the *Retrieval Manager* to which the query is directed contain links that reference another *Retrieval Manager*. For these links a subquery has to be formed by the first *Retrieval Manager* and passed to the next *Retrieval Manager*. At the second *Retrieval Manager* this process can be repeated.

First let us define a term that will give the around–the–loop time for a subquery:

$$t_{sum} = t_{fill}^{forward} + t_{xmit}^{forward} + t_{local,col} + t_{fill}^{reply} + t_{xmit}^{reply}$$

Next we need to recognize that one of the devices involved forms the longest portion of the around–the–loop time:

$$t_{max} = \text{maximum}(t_{fill}^{forward}, t_{fill}^{reply}, t_{xmit}^{forward}, t_{xmit}^{reply}, t_{local,col})$$

With the two values calculated above we can calculate the average response time to a distributed collection search:

$$t_{dist,col} = t_{local,col} + R/(1 - R) \times \left(t_z + \left(t_{sq} \times A/2 \right) + \left(t_{max} \times R \times A \right) / (N_{sites} - 1) + (t_{sum} - t_{max}) \right)$$

This equation may need to be revised if it is determined that the network connection between *Retrieval Managers* can handle multiple messages simultaneously.

8.3.4 Distributed Product Description Searches

Because of the way that searches were subdivided, the equation for the average response time to a distributed product description query is:

$$t_{dist,prod} = t_{dist,col} + (1 - O_{col}) \times A^{depth/2} \times \left(d_{xlate} / (1 - \rho_{xlate}) + d_{inv} / (1 - \rho_{inv}) \right)$$

The network time caveat stated in Section 8.3.2 holds here as well.

8.3.5 Parameters Used for Performance Estimation

Table 8-6 defines the parameters used in estimating query performance within ICS. Included in the table are the units and the nominal values used for estimation. For some parameters the nominal value is marked "dev." This indicates that the value of the parameter is developed (estimated via the equations given above) rather than being an input parameter.

Table 8-6. Definition of Performance Parameters

Name	Value	Units	Definition
A	TBD	n/a	The average number of collections per collection
d_{col}	dev.	seconds	Average collection query service time
d_{inv}	TBD	seconds	Average inventory (catalogue) query service time
d_{xlate}	TBD	seconds	Average catalogue translation service time
depth	TBD	n/a	The average collection depth of the collections held by a specific *Retrieval Manager*.
N_{sites}	13	n/a	Number of ICS sites (number of *Retrieval Managers*)
O_{col}	TBD	n/a	Probability that a collection will overlap another collection
R	TBD	n/a	Ratio of the number of remote links to the total number of collection-to-collection links.
ρ_{inv}	0.5	n/a	Inventory Catalogue System utilization (traffic intensity).
ρ_{RM}	0.5	n/a	*Retrieval Manager* utilization (traffic intensity).
ρ_{xlate}	0.5	n/a	*Catalogue Translator* utilization (traffic intensity).
$t_{dist,col}$	dev.	seconds	The average time required to perform a distributed collection search.
$t_{dist,prod}$	dev.	seconds	The average time required to perform a distributed product search.
t_{fill}	TBD	seconds	The average time required to pass a query message (forward) or a response to a query (reply) to the networks.
$t_{local,col}$	5	seconds	The average time required to search a local collection.
$t_{local,prod}$	dev.	seconds	The average time required to perform a local product description search.
t_{sq}	TBD	seconds	The average time required to form a subquery from a query
t_{xmit}	TBD	seconds	The average time elapsed while the networks to transmit a message to its final destination.
t_z	TBD	seconds	The average time required to establish a Z–association.

9. ICS COMPATABILITY AND CONFIGURATIONS

This section defines the required configuration for sites which wish to be considered ICS compatible. Recognizing that the configuration of ICS sites will vary, this section provides a range of configurations. Each configuration is defined by indicating the level of SDD compatibility required of the site in the following dimensions: provision of ICS elements, CIP messages supported, ICS data required, ICS operations supported by the site, and compatibility with SDD Paragraphs.

Note that this section does not define CIP Compatibility, which is defined in the CIP Specification [R3]. The relationship between CIP and ICS compatibility is addressed in Sections 1.1 and 2.1.3 of the SDD.

9.1 Canonical ICS Sites

There will be many different variations on how agencies chose to implement ICS sites. This section defines three canonical sites which are used in the remainder of this chapter. Two extreme cases and one moderate implementation are defined as follows:

- **Minimum CEOS ICS Site**. CEOS policy anticipates that members will provide the following: collection and product searches, explain
- **Moderate ICS Site.** In addition to the services provided by a minimum CEOS ICS site as listed above, this canonical ICS site provides limited ordering services. Ordering is limited to non-authenticated, direct ordering. This site also has greater system management capabilities.
- **Maximum ICS Site.** This implementation provides all features, elements, messages and services which are defined in the ICS SDD.

Two other site implementations involve less than a ICS site and are described here as exceptions: Retrieval Manager as a Router site and a Catalogue Translator Only site. The Retrieval Manager as a Router is shown in Figure 3-3 and would be an exceptional site as the functionality provided is very limited. A site may also be implemented with just a Catalogue Translator which is served by a Retrieval Manager at another site. The site's collections are listed in the Retrieval Manager, and product searches of the collections are passed from the Retrieval Manager to the Catalogue Translator. This allows the Translator-only site to dynamically change its product holdings and be visible in ICS without having to host a Retrieval Manager. This configuration is discussed in Section 3-2 where a Retrieval Manager is shown serving multiple Translators. These configurations are not addressed as a canonical site.

9.2 Element Identification

This section provides an itemization of all Elements which constitute the ICS. This identification facilitates the collaborative development of ICS Elements. An indication will be provided as to the development heritage of the Elements, e.g., new development, existing standard, reuse, COTS, etc. See the PTT Plan [R1] for information on the availability of ICS elements.

Identification of the ICS Element and their development heritage is provided in Table 9-1.

Table 9-1. ICS Element Identification and Heritage

Element Number	Element Name	Heritage of Element
ICS-01	Retrieval Manager	New Development: CEO CIP Demonstrator DBV-OSI for z39.50 API
ICS-02	CIP Client Application	New Development: CEO CIP Demonstrator DBV-OSI for z39.50 API
ICS-03	Catalogue Translator	New Development: "skeleton" translator from CEO CIP Demonstrator
ICS-04	OHS Translator	New Development:
ICS-05	UPS Translator	New Development:
ICS-06	HTTP/CIP Gateway	New Development: CEO CIP Demonstrator CINTEX WWW Gateway
ICS-07	Collection Management Tools (CMT)	New Development: TBD
ICS-08	Monitoring and Control Tools (MCT)	New Development: TBD
ICS-09	ICS Gateway	New Development: TBD
Not applicable	Retrieval Manager Administrator (RMA)	Not applicable. (Note: a Collections Manual and Administration Manual are envisioned in the PTT plan.)

Identification of ICS Related Elements and their development heritage is in provided in Table 9-2.

Table 9-2. ICS Related Elements

Element Number	Element Name	Heritage of Element
Site Specific	Order Handling System	
Site Specific	Data Archive	
Site Specific	User Profile System	
Site Specific	Existing Catalogue	

9.3 Compatibility Definitions

The next sections use the following terminology to describe the compatibility of a site with the SDD.

- **Mandatory** - A site must comply with the listed item, e.g., provision of an element at a site or contents of an SDD paragraph.
- **Mandatory As Applicable (MAA)** - If the site is implementing the item, then the site must comply with the applicable portions.
- **Suggested** - A site should comply with the item.
- **Explanatory** - The listed item is an ICS concept: a site need not explicitly comply with the item.
- **Not Applicable** - A site need not comply with the item.

9.4 ICS Elements by Canonical Site

For the three canonical ICS site configurations, an identification of the required conformance of a site in providing ICS elements is listed in Table 9-3.

Table 9-3. ICS Elements by Canonical Site

Element Name	Minimum Site	Moderate Site	Maximum Site
Retrieval Manager	MAA	MAA	Mandatory
CIP Client Application	MAA	MAA	Mandatory
Catalogue Translator	Suggested	Suggested	Mandatory
OHS Translator	Not Applicable	MAA	Mandatory
UPS Translator	Not Applicable	MAA	Mandatory
HTTP/CIP Gateway	Suggested	MAA	Mandatory
ICS Gateway	Suggested	Suggested	Mandatory
RMA	Mandatory	Mandatory	Mandatory
CMT	Suggested	MAA	Mandatory
MCT	Suggested	MAA	Mandatory
Existing Catalogue	Suggested	Suggested	Mandatory
Order Handling System	Not Applicable	MAA	Mandatory
User Profile System	Not Applicable	MAA	Mandatory
Data Archive	MAA	MAA	Mandatory

9.5 CIP Messages by Canonical Site

For the three canonical ICS site configurations, an identification of the required services which the Retrieval Manager at the site will support are listed in Table 9-4.

Moderate site will include persistent results sets, database update and persistent queries. It does not include: periodic query and CIP ordering.

Table 9-4. CIP Messages by Canonical Site

CIP Message Name	Minimum Site	Moderate Site	Maximum Site
initializeRequest	Mandatory	Mandatory	Mandatory
initializeResponse	Mandatory	Mandatory	Mandatory
searchRequest	Mandatory	Mandatory	Mandatory
searchResponse	Mandatory	Mandatory	Mandatory
presentRequest	Mandatory	Mandatory	Mandatory
presentResponse	Mandatory	Mandatory	Mandatory
segmentRequest	Mandatory	Mandatory	Mandatory
DeleteResultSetRequest	Mandatory	Mandatory	Mandatory
DeleteResultSetResponse	Mandatory	Mandatory	Mandatory
AccessControlRequest	Suggested	Suggested	Mandatory
AccessControlResponse	Suggested	Suggested	Mandatory
ResourceControlRequest	Suggested	Suggested	Mandatory
ResourceControlResponse	Suggested	Suggested	Mandatory
TriggerResourceControlRequest	Suggested	Suggested	Mandatory
ResourceReportRequest	Suggested	Suggested	Mandatory
ResourceReportResponse	Suggested	Suggested	Mandatory
ExtendedServicesRequest	MAA	MAA	Mandatory
ExtendedServicesResponse	MAA	MAA	Mandatory
close	Mandatory	Mandatory	Mandatory

9.6 ICS Data by Canonical Site

For the three canonical ICS site configurations, an identification of the required operations which the personnel at the site must provide are listed in Table 9-5.

Table 9-5. ICS Data by Canonical Site

Element Name	Minimum Site	Moderate Site	Maximum Site
CDB	Mandatory	Mandatory	Mandatory
Extended Services Database	MAA	MAA	Mandatory
Explain Database	Mandatory	Mandatory	Mandatory
Session Management Data	Mandatory	Mandatory	Mandatory
Error Management Data	Suggested	Mandatory	Mandatory
User Management Data	Mandatory	Mandatory	Mandatory

9.7 ICS Operations by Canonical Site

For the three canonical ICS site configurations, an identification of the required operations which the personnel at the site must provide are listed in Table 9-6.

Table 9-6. ICS Operations by Canonical Site

Element Name	Minimum Site	Moderate Site	Maximum Site
Retrieval Manager nominal operations: 24 hours per day, 7 days per week.	Mandatory	Mandatory	Mandatory
Trained RMA Staff: operations staff at the site trained as ICS RMAs.	Mandatory	Mandatory	Mandatory
RMA Response Time: maximum time for RMA at a site to begin responding to an ICS Event	4 hours	4 hours	15 minutes
Perform Collection Maintenance as defined in ICS Collection Manual	MAA	MAA	Mandatory
Security information management	Not Applicable	Not Applicable	Mandatory
Interagency Agreements for Indirect Ordering	Not Applicable	Not Applicable	Mandatory
Site is able to perform system-wide ICS System Management	Not Applicable	Not Applicable	Suggested

9.8 SDD Paragraph by Canonical Site

This section provides indicates the applicable paragraphs of the SDD which a site needs to be compliant. The matrix in this section (Table 9-7) indicates which sections are mandatory and which are not mandatory for ICS compatibility.

Table 9-7. SDD Paragraph Applicability to Canonical Site (1 of 2)

SDD Paragraph	Minimum Site	Moderate Site	Maximum Site
1. INTRODUCTION	Explanatory	Explanatory	Explanatory
2. ICS DESIGN APPROACH	Explanatory	Explanatory	Explanatory
3. FUNCTIONAL VIEW			
3.1 Architecture Foundations	Explanatory	Explanatory	Explanatory
3.2 ICS Functional Framework	MAA	MAA	Mandatory
3.3 Catalogue Interoperability Protocol (CIP)	MAA	MAA	Mandatory
3.4 CIP Operations			
3.4.1 Queries			
3.4.1.1 Local Query	Mandatory	Mandatory	Mandatory
3.4.1.2 Distributed Query	MAA	MAA	Mandatory
3.4.2 Ordering of EO Products			
3.4.2.1 Direct Ordering	Not Applicable	Mandatory	Mandatory
3.4.2.2 Indirect Ordering	Not Applicable	Not Applicable	Mandatory
3.5 Identification of ICS Element Services and Interfaces			
3.5.1 Retrieval Manager Services	MAA	MAA	Mandatory
3.5.2 CIP Client Application Services	MAA	MAA	Mandatory
3.5.3 Catalogue Translator Services	MAA	MAA	Mandatory
3.5.4 OHS Translator Services	MAA	MAA	Mandatory
3.5.5 UPS Translator Services	MAA	MAA	Mandatory
3.5.6 HTTP/CIP Gateway Services	MAA	MAA	Mandatory
3.5.7 ICS Gateway	Suggested	Suggested	Suggested
3.5.8 Retrieval Manager Administrator (RMA) Operations	MAA	MAA	Mandatory
3.5.9 Collection Management Tools (CMT) Services	Suggested	MAA	Mandatory
3.5.10 Monitoring and Control Tools (MCT) Services	Suggested	MAA	Mandatory
3.6 Identification of ICS Related Element Services	Suggested	Suggested	Suggested
4. DATA VIEW			
4.1 Collection Concept	Explanatory	Explanatory	Explanatory
4.2 Collection Concept Details	Explanatory	Explanatory	Explanatory
4.3 ICS Data Framework	MAA	MAA	Mandatory
4.4 Collection Database(CDB)	Mandatory	Mandatory	Mandatory
4.5 Explain Database	Mandatory	Mandatory	Mandatory
4.6 Extended Services Database	Suggested	Mandatory	Mandatory
4.7 Session Management Database	Mandatory	Mandatory	Mandatory
4.8 Error Management Database	Mandatory	Mandatory	Mandatory

Table 9-8. SDD Paragraph Applicability to Canonical Site (2 of 2)

SDD Paragraph	Minimum Site	Moderate Site	Maximum Site
4.9 User Management Database	Suggested	Mandatory	Mandatory
4.10 Global Node Data Architecture	Not Applicable	Not Applicable	MAA
4.11 Collection Census	Explanatory	Explanatory	Explanatory
4.12 Data in Other ICS Elements	MAA	MAA	Mandatory
5. COMMUNICATIONS VIEW			
5.1 ICS Communication Framework			
5.1.1 TCP/IP Services	Explanatory	Explanatory	Explanatory
5.1.2 CIP Translators and TCP Communication Stack	MAA	MAA	Mandatory
5.1.3 Implementing CIP using TCP/IP Services	Mandatory	Mandatory	Mandatory
5.1.4 Distributed Session Management	MAA	Mandatory	Mandatory
5.1.5 Directory Services	Mandatory	Mandatory	Mandatory
5.2 CEOS Network Connectivity	Suggested	Suggested	Mandatory
6. SECURITY VIEW			
6.1 ICS Security Assessment	Explanatory	Explanatory	Explanatory
6.2 ICS Secure System Design			
6.2.1 Administrative Security Controls	Suggested	MAA	Mandatory
6.2.2 Physical Security Control	Suggested	Suggested	Suggested
6.2.3 Computing Security Controls			
6.2.3.1 Summary of Computing Security Controls	MAA	MAA	Mandatory
6.2.3.2 Authentication Mechanism	Not Applicable	Not Applicable	Mandatory
6.2.3.3 Group Security Model	Not Applicable	Not Applicable	Mandatory
6.2.3.4 Group Management	Not Applicable	Not Applicable	Mandatory
7. SYSTEM MANAGEMENT VIEW	Explanatory	Explanatory	Explanatory
8. ARCHITECTURE VERIFICATION			
8.1 Scenarios			
8.1.1 User Scenarios	Suggested	Suggested	Suggested
8.1.2 Collection Population Scenarios	Suggested	Suggested	Suggested
8.1.3 System Management Scenarios	Explanatory	Explanatory	Explanatory
8.2 Internal Interface Identification	MAA	MAA	Mandatory
8.3 Query Performance Estimates	Explanatory	Explanatory	Explanatory
9. ICS COMPATABILITY AND CONFIGURATIONS	Mandatory	Mandatory	Mandatory

9.9 Open Issues List

This section contains a list of items which are known to be incomplete or are planned for future versions of the document.

1) Section 7, System Management. Currently section 7 contains a list of items related to system management which were identified during the development of other parts of the document. A comprehensive design approach to the ICS System Management will be provided in a future version of this document.

2) Section 9, ICS Compatibility and Configurations. Method of presenting the compatibility approach, i.e., the tables in Section 9, may need to be revised if the approach does not provide a definitive statement of what it means for a site to be compatible.

3) Section 9, ICS Compatibility and Configurations. The definition of a moderate site in Section 9.1 should be reviewed based on implementation experience of ICS sites.

4) New Section, Traceability Matrix. Provide a traceability matrix mapping from ICS URD requirements to ICS SDD sections.

5) Performance Modeling. CEOS network bandwidth and performance estimates based on modeling estimate are incomplete. Several modeling input parameters are to be provided to the PTT based on the CEO CIP-A Demonstrator (See PTT-4 Action Item). When the parameters are available, the estimates can be completed and the missing entries can be supplied for Sections 5.2.3 and 8.3.

6) Indirect Ordering. For ordering, a *Retrieval Manager* will need to know if the order is placed by another *Retrieval Manager*, i.e., an indirect order, or by a user, i.e., a direct order. During PTT-4 an action was assigned to answer this need by a special syntax for the user ID of a Retrieval Manager. As many sites will not have the liberty to assign user IDs with a special ICS defined syntax, an alternate approach will need to be developed for CIP ordering.

7) Review Sections 3 and 4 with the PTT Engineering Core team on the topic of handling Extended Services. Address the coordination of related task packages stored in multiple ICS elements, e.g., Retrieval Managers and OHS Translators. This issue was previously the PTT Action Item 961204/5 identified during PTT-4 in Ispra.